Cyber S&T Priority Steering Council Research Roadmap

for the

National Defense Industrial Association Disruptive Technologies Conference

8 November 2011

Steven E. King, Ph.D.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **08 NOV 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Cyber S& T Priority Steering Council Research Roadmap**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Washington,DC,20310**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

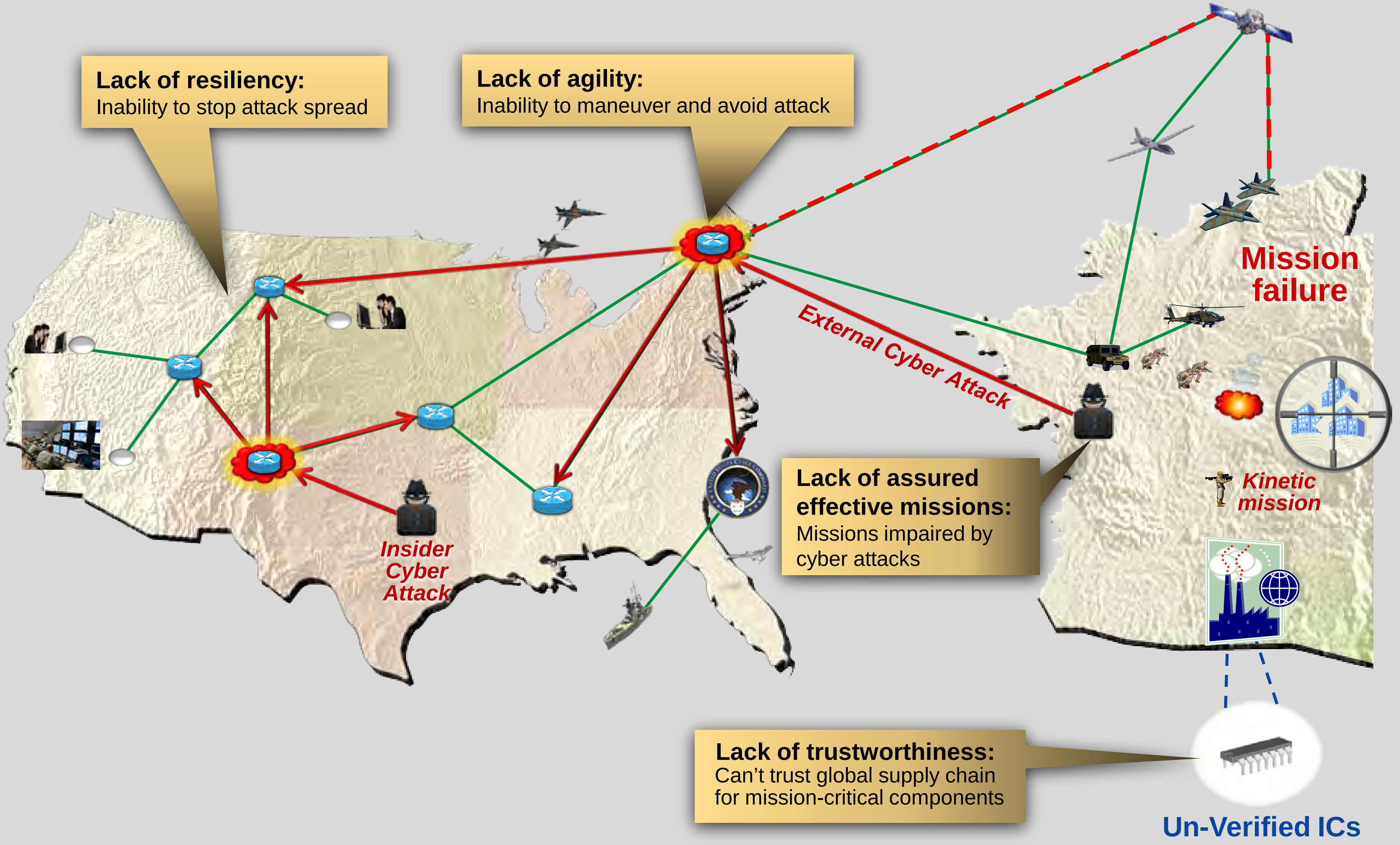
13. SUPPLEMENTARY NOTES
Presented at the NDIA Disruptive Technologies Conference, November 8, 2011 Washington, DC

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

Problem Statement



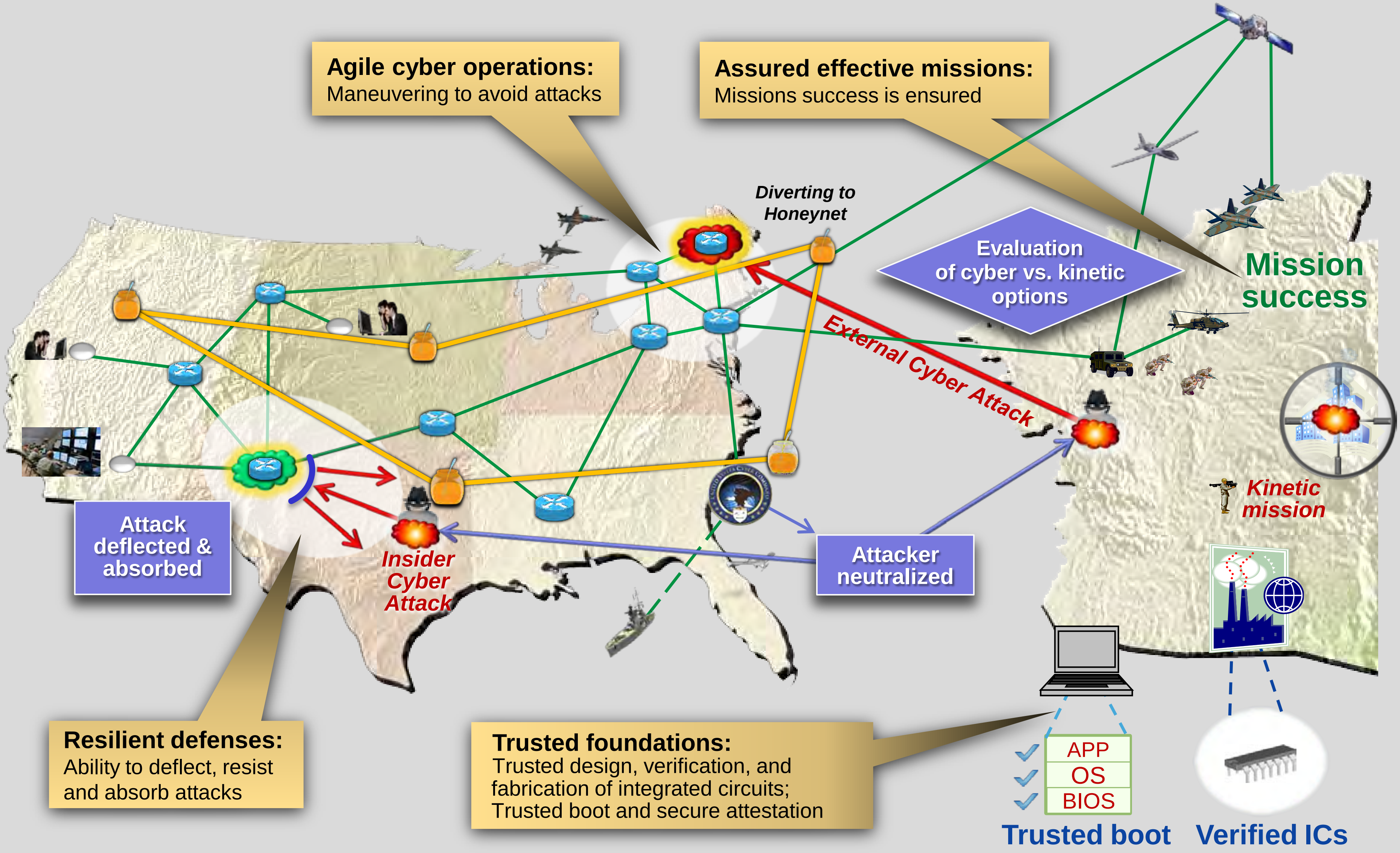
Lack of resiliency:
Inability to stop attack spread

Lack of agility:
Inability to maneuver and avoid attack

Lack of assured effective missions:
Missions impaired by cyber attacks

Lack of trustworthiness:
Can’t trust global supply chain for mission-critical components

Desired End State



Agile cyber operations:
Maneuvering to avoid attacks

Assured effective missions:
Missions success is ensured

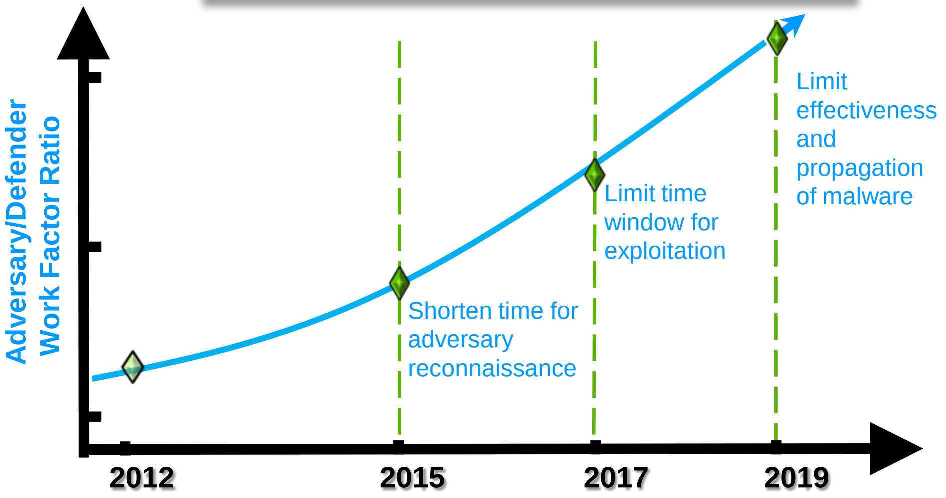
Resilient defenses:
Ability to deflect, resist and absorb attacks

Trusted foundations:
Trusted design, verification, and fabrication of integrated circuits;
Trusted boot and secure attestation

Key Parameter: Work Factor Ratio

- **Missions**
  - Kinetic, cyber, and combined missions will have a cyber dependency
- **Infrastructure**
  - Any element of the cyber infrastructure may be compromised and manipulated
  - DoD will continue to leverage commercial products and services we do not own or control
  - DoD infrastructure defies establishing an all-encompassing static perimeter

Challenge: Increase Adversary / Defender Relative Work Factor Over Time



Shorten time for adversary reconnaissance

Limit time window for exploitation

Limit effectiveness and propagation of malware

Perimeter is not well defined

Distribution Statement A: Approved for public release; distribution is unlimited.

Four Major 10 Year Objectives

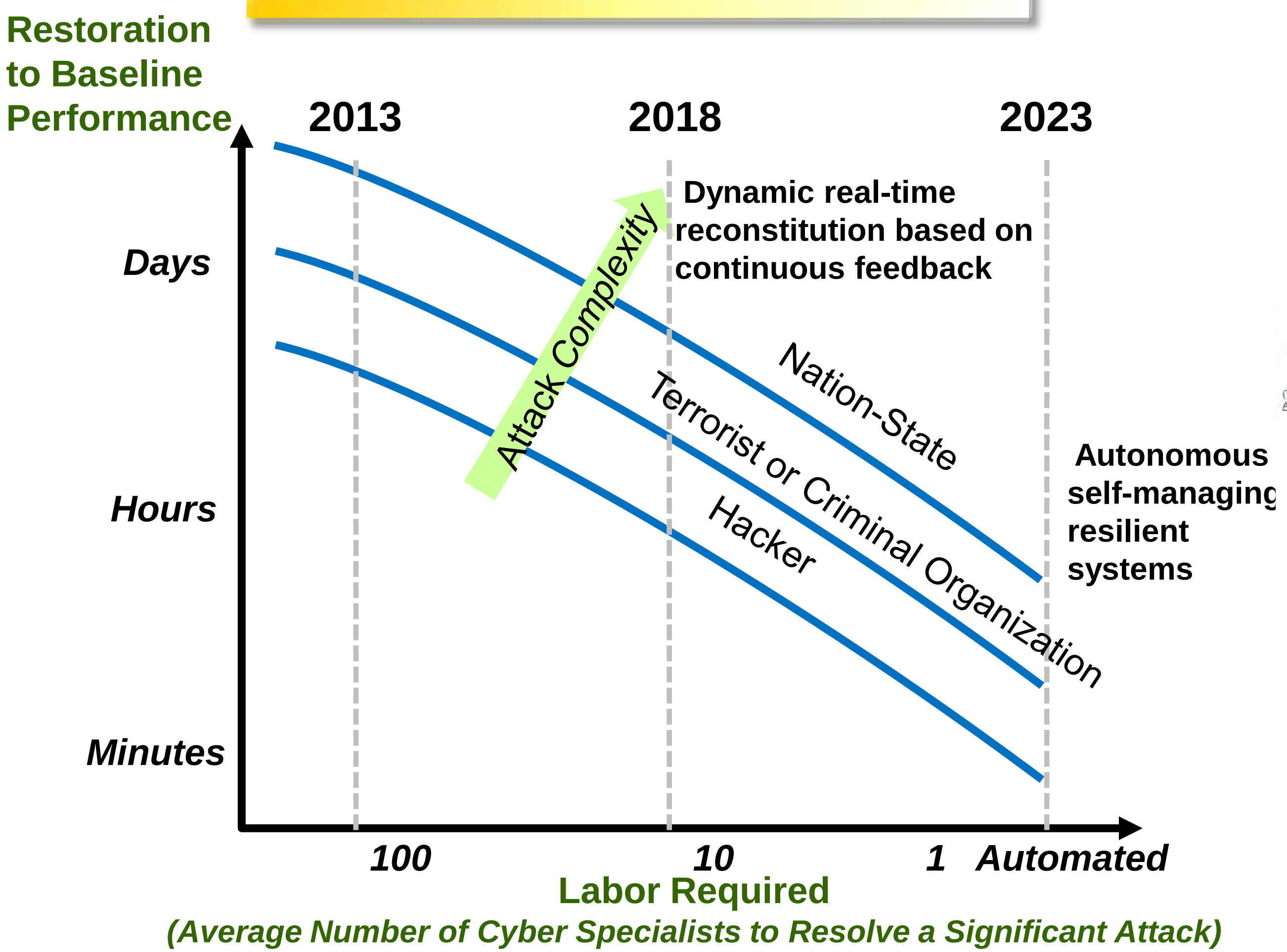
Assuring Effective Missions	Assess and control the cyber situation in mission context
Agile Operations	Dynamically reshape cyber systems as conditions/goals change, to escape harm

Resilient Infrastructure	Withstand cyber attacks, and sustain or recover critical functions
Trust	Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

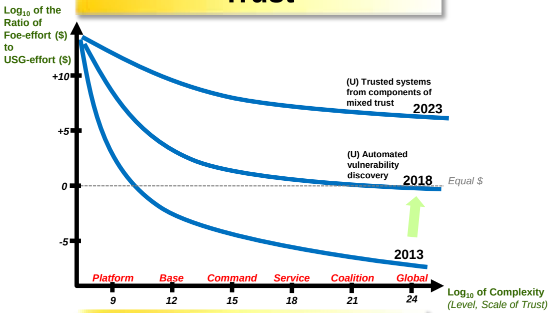
Distribution Statement A: Approved for public release; distribution is unlimited.

Metrics

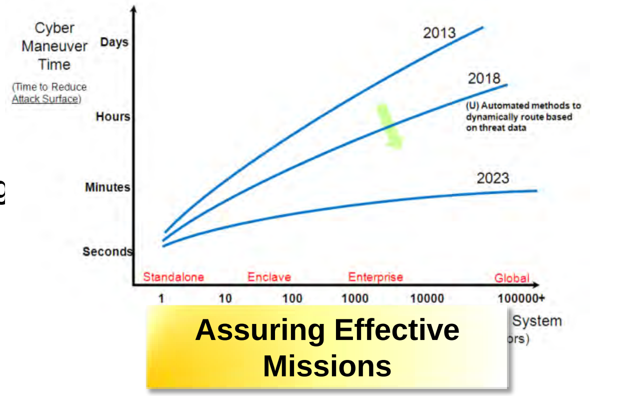
Resilient Infrastructure



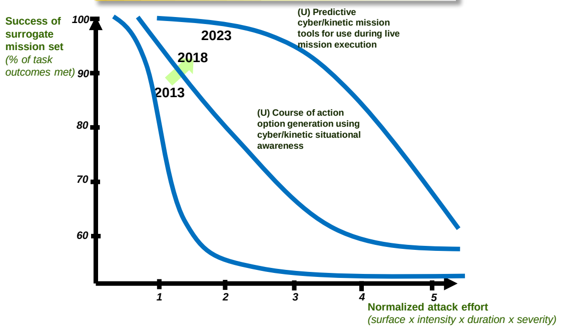
Trust



Operational Agility



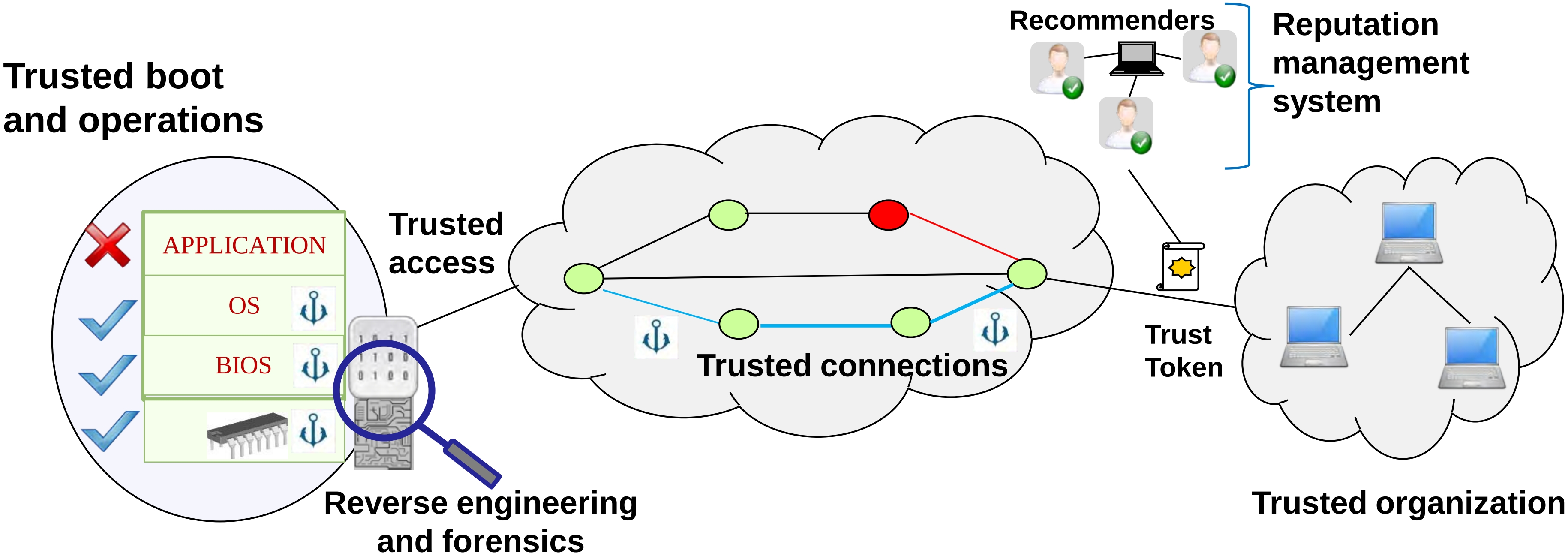
Assuring Effective Missions



Distribution Statement A: Approved for public release; distribution is unlimited.

Trust

Technical Challenges and Research Opportunities



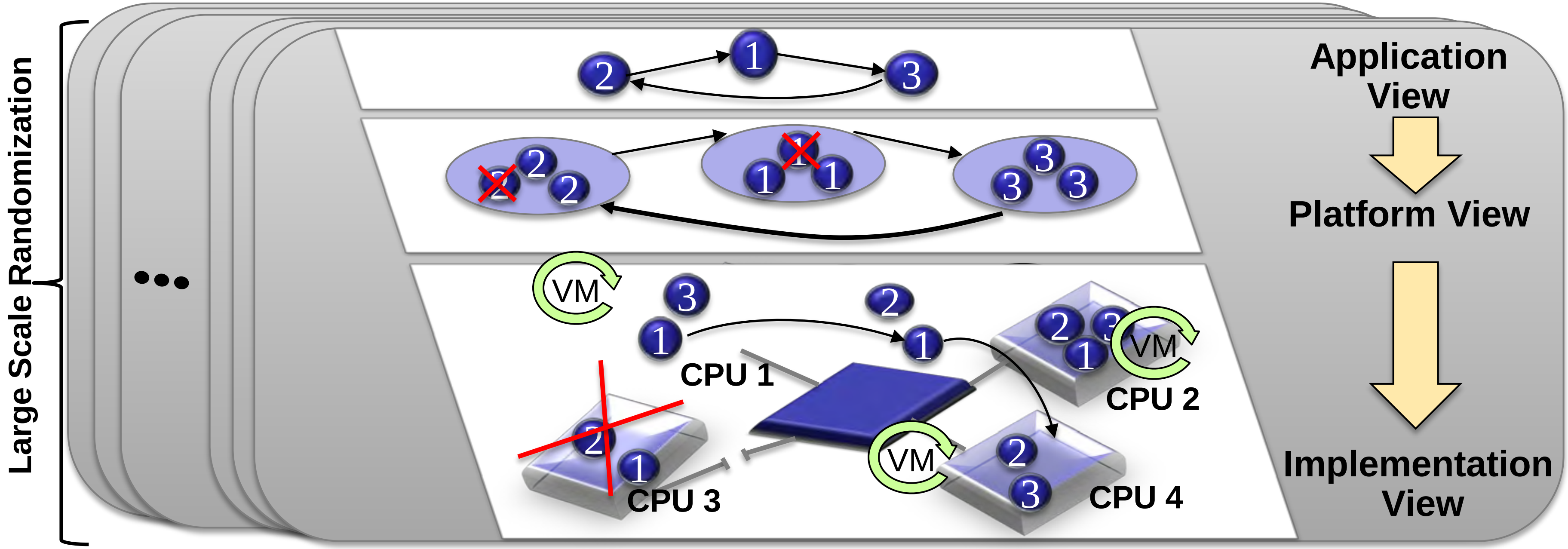
Trust Foundations

- Scalable reverse engineering and analysis
- Trust establishment, propagation, and maintenance techniques
- Measurement of trustworthiness
- Trustworthy architectures and trust composition tools

Distribution Statement A: Approved for public release; distribution is unlimited.

Resilient Infrastructure

Technical Challenges and Research Opportunities



Resilient Architectures

- Resiliency for operational systems
- Mechanisms to compose resilient systems from brittle components
- Integration of sensing, detection, response, and recovery mechanisms
- Secure modularization and virtualization of nodes and networks
- Resiliency-specific modeling and simulation

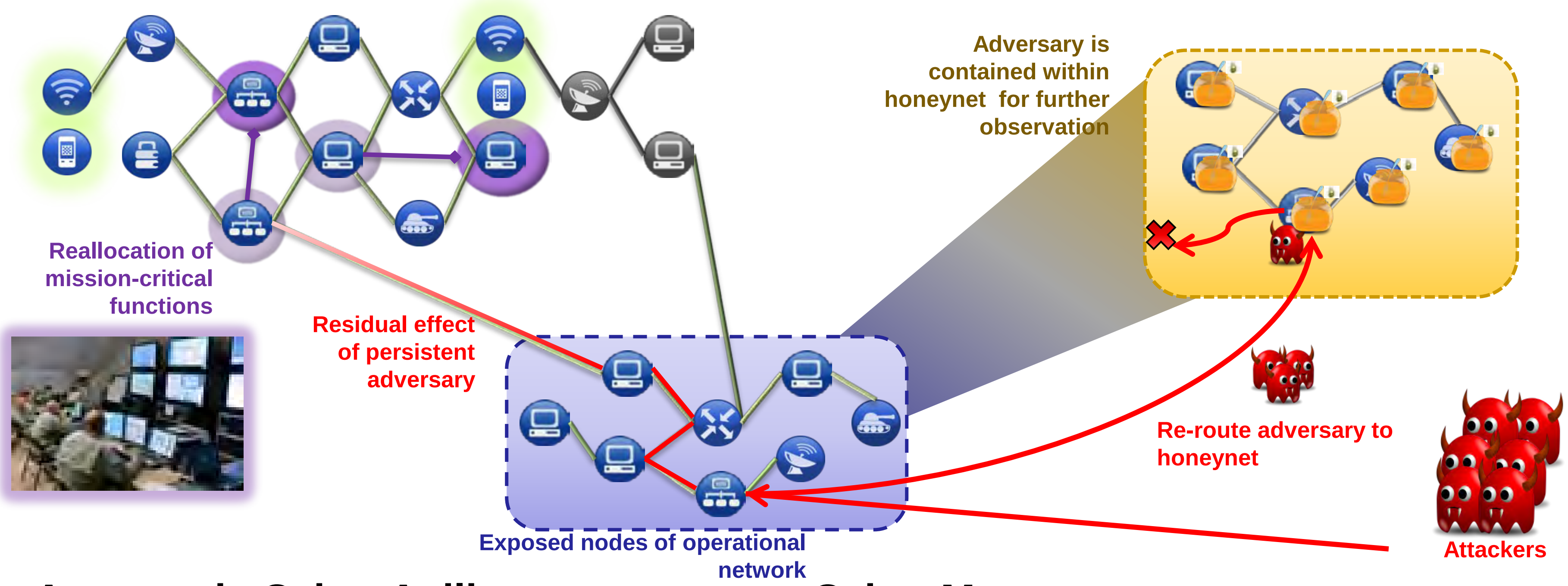
Resilient Algorithms and Protocols

- Code-level software resiliency
- Network overlays and virtualization
- Network management algorithms
- Mobile computing security

Distribution Statement A: Approved for public release; distribution is unlimited.

Agile Operations

Technical Challenges and Research Opportunities


Adversary is contained within honeynet for further observation
Reallocation of mission-critical functions
Residual effect of persistent adversary
Re-route adversary to honeynet
Exposed nodes of operational network
Attackers

Autonomic Cyber Agility

- Techniques for autonomous reprogramming, reconfiguration, and control of cyber components
- Machine intelligence and automated reasoning techniques for executing courses of action

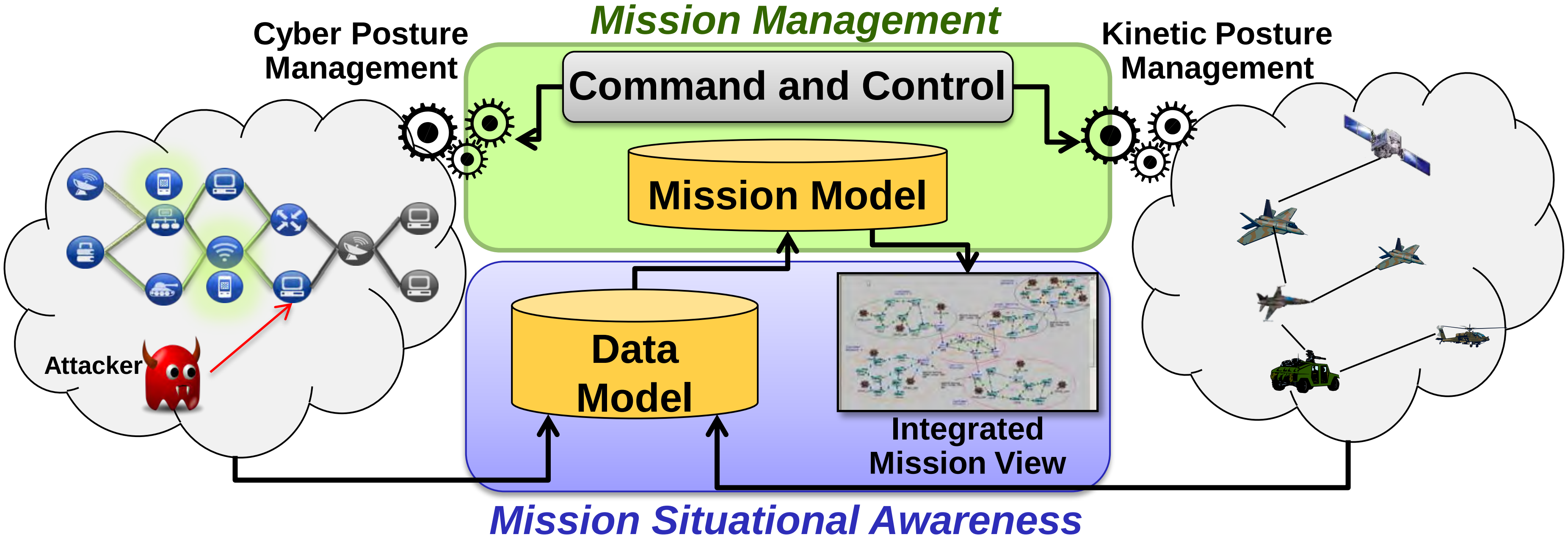
Cyber Maneuver

- Distributed systems architectures and service application polymorphism
- Network composition based on graph theory
- Distributed collaboration and social network theory

Distribution Statement A: Approved for public release; distribution is unlimited.

Assuring Effective Missions

Technical Challenges and Research Opportunities



Cyber Mission Control

- Techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure
- Techniques for course of action development and analysis
- Cyber effects assessment

Distribution Statement A: Approved for public release; distribution is unlimited.

Open Broad Agency Announcements

- **Army Research Office (ARO)**
  - Solicitation #:W911NF-07-R-0003-04; BAA for Basic and Applied Research, Section 5.3
- **Army Research Laboratory (ARL)**
  - Solicitation #:W911NF-07-R-0001-05; BAA for Basic and Applied Research, Section 1
- **Communications and Electronics Research, Development, and Engineering Center (CERDEC)**
  - Solicitation #: W15P7T-08-R-P415
- **Office of Naval Research (ONR)**
  - Solicitation #: ONRBAA 12-001, Code 31 Section 1
- **Naval Research Laboratory (NRL)**
  - Solicitation #: BAA-N00173-02, Section 55-11-02 (Mathematical Foundations of Computing)
  - Solicitation #: BAA-N00173-02, Section 55-11-03 (High Assurance Engineering and Computing)
- **Air Force Office of Scientific Research (AFOSR)**
  - Solicitation #: AFOSR-BAA-2010-1, Section c.12
- **Air Force Research Laboratory (AFRL)**
  - Solicitation #: BAA-10-09-RIKA (Cross Domain Innovative Technologies)
  - Solicitation #: BAA-11-01-RIKA (Cyber Assurance Technologies)
- **Defense Advanced Research Projects Agency (DARPA)**
  - Solicitation #: DARPA-BAA-11-63 (Automated Program Analysis for Cyber Security)
  - Solicitation #: DARPA-BAA-10-83 (Strategic Technologies Office BAA)
  - Solicitation #: DARPA-BAA-11-34 (Information Innovation Office BAA)
  - Solicitation #: DARPA-RA-11-52 (Cyber Fast Track)
  - Solicitation #: DARPA-SN-11-55 (Future Directions in Cyber Security)

Small Business Innovation Research Announcements

http://www.dodsbir.net

NSA Contact Information

(No Open BAAs)

Acquisition Resource Center
Phone: (443)-479-9572
E-mail: nsaarc@nsaarc.net

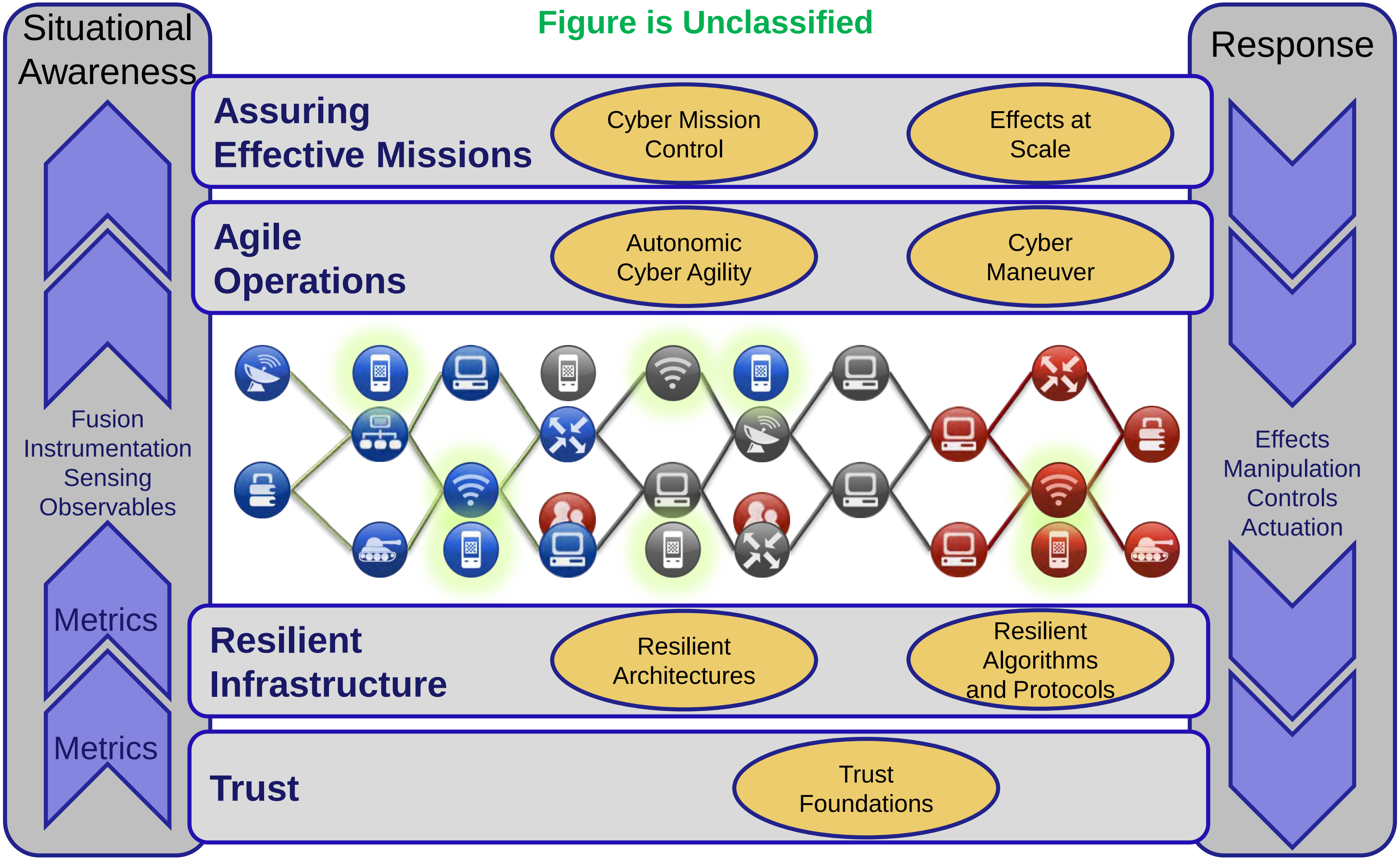
Office of Small Business Programs
Phone: (443)-479-9572
E-mail: nsaarc@nsaarc.net

Distribution Statement A: Approved for public release; distribution is unlimited.

Technology Challenge Summary

POC: Dr. Steven E. King

Figure is Unclassified



Situational Awareness

Fusion
Instrumentation
Sensing
Observables

Metrics

Metrics

Assuring Effective Missions

Cyber Mission Control

Effects at Scale

Agile Operations

Autonomic Cyber Agility

Cyber Maneuver

Resilient Infrastructure

Resilient Architectures

Resilient Algorithms and Protocols

Trust

Trust Foundations

Response

Effects
Manipulation
Controls
Actuation

Distribution Statement A: Approved for public release; distribution is unlimited.